5312579.

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
6. Mai 2004 (06.05.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/038665 A1

(51) Internationale Patentklassifikation[7]: G07F 7/10

(21) Internationales Aktenzeichen: PCT/EP2003/011761

(22) Internationales Anmeldedatum:
23. Oktober 2003 (23.10.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 49 801.6 24. Oktober 2002 (24.10.2002) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81667 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **MEISTER, Gisela** [DE/DE]; Stademannstrasse 11, 81737 München (DE). **MARTIN, Nigol** [DE/DE]; Astallerstrasse 12, 80339 München (DE).

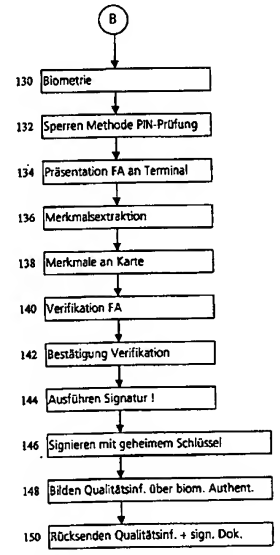
(74) Anwalt: **KLUNKER, SCHMITT-NILSON, HIRSCH**; Winzererstrasse 106, 80797 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT,

*[Fortsetzung auf der nächsten Seite]*

(54) Title: METHOD FOR CARRYING OUT A SECURE ELECTRONIC TRANSACTION USING A PORTABLE DATA SUPPORT

(54) Bezeichnung: VERFAHREN ZUM AUSFÜHREN EINER GESICHERTEN ELEKTRONISCHEN TRANSAKTION UNTER VERWENDUNG EINES TRAGBAREN DATENTRÄGERS




130:- BIOMETRY
132:- LOCK METHOD PIN CHECKING
134:- PRESENTATION OF FINGERPRINT TO THE TERMINAL
136:- FEATURE EXTRACTION
138:- FEATURES TO THE CARD
140:- FINGERPRINT VERIFICATION
142:- CONFIRM VERIFICATION
144- CARRY OUT SIGNATURE
146:- SIGN WITH SECRET CODE
148:- FORM QUALITY INFORMATION BY MEANS OF BIOMETRIC AUTHENTIFICATION
150:- RETURN QUALITY INFORMATION AND SIGNED DOCUMENT

(57) **Abstract:** A method for carrying out a secure electronic transaction on a terminal using a portable data support is disclosed. According to the invention, a user (30) first authenticates themselves to the portable data support (20). The portable data support (20) generates quality information (20) on how the authentification occurred, which is verified for the terminal (14). The portable data support (20) then carries out a security-based operation within the context of the transaction, for example, the generation of a digital signature. The result of the security-based operation is added to the quality information.

(57) **Zusammenfassung:** Vorgeschlagen wird ein Verfahren zum Ausführen einer gesicherten elektronischen Transaktion an einem Terminal unter Verwendung eines tragbaren Datenträgers. Verfahrensgemäß authentifiziert sich zunächst ein Nutzer (30) gegenüber dem tragbaren Datenträger (20). Dabei erzeugt der tragbare Datenträger (20) eine Qualitätsinformation darüber, auf welche Weise die Authentifizierung erfolgte. Die Authentifizierung wird dem Terminal (14) bestätigt. Anschließend führt der tragbare Datenträger (20) im Rahmen der Transaktion eine sicherheitsbegründende Operation aus, beispielsweise die Erstellung einer digitalen Signatur. Dem Ergebnis der sicherheitsbegründenden Operation fügt er die Qualitätsinformation bei.

WO 2004/038665 A1

RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Bestimmungsstaaten** *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Veröffentlicht:**
— *mit internationalem Recherchenbericht*
— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

*Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.*

# Verfahren zum Ausführen einer gesicherten elektronischen Transaktion unter Verwendung eines tragbaren Datenträgers

Die Erfindung geht aus von einem Verfahren nach der Gattung des Hauptanspruchs. Ein solches ist zum Beispiel aus dem „Handbuch der Chipkarten", W. Rankl, W. Effing, 3. Auflage, 1999, S. 692 bis703 unter dem Titel „Digitale Signatur" bekannt. Zur Vornahme einer rechtsverbindlichen elektronischen Signatur soll danach eine digitale Signaturkarte eingesetzt werden, auf der sich ein geheimer Signaturschlüssel befindet. Die Vornahme einer Signatur erfolgt an einem geeigneten Terminal, von dem die Karte ein zu signierendes Dokument in elektronischer Form erhält. Um eine Signatur vornehmen zu können, muß der Nutzer der Karte über das Terminal seine Identität nachweisen. Regelmäßig erfolgt dieser Nachweis durch Eingabe einer PIN (Personen-Identifikations-Nummer), welche mit einer in der Karte gespeicherten Referenz-PIN verglichen wird. Zukünftig ist vorgesehen, die Nutzerauthentifizierung durch Prüfung eines biometrischen Merkmales, etwa eines Fingerabdruckes, vorzunehmen. Wurde ein elektronisches Dokument nach erfolgreicher Authentifizierung des Nutzers mit Hilfe einer Signaturkarte signiert, kann es anschließend auf beliebige Weise weitergegeben werden. Mit Hilfe der elektronischen Signatur wird es möglich, besonders sicherheitskritische Transaktionen, etwa die Erteilung von kostenbehafteten Dienstleistungsaufträgen, auf elektronischem Wege durchzuführen.

Durch die beabsichtigte Einführung biometrischer Merkmale zur Benutzerauthentifizierung wird eine weitere Verbesserung der Vertrauenswürdigkeit einer elektronischen Signatur gegenüber der bislang üblichen PIN-Authentifizierung erreicht, weil dadurch sichergestellt ist, daß eine Benutzung der Signaturkarte nur in Anwesenheit einer definierten, dazu berechtigten Person erfolgen kann.

Der hierin verwirklichte Qualitätsunterschied hinsichtlich der Nutzerauthentifizierung findet in der Nutzbarkeit der jeweils erzeugten elektronischen Signatur bislang jedoch keinen Niederschlag.

Es ist Aufgabe der Erfindung, ein Verfahren zum Ausführen einer gesicherten elektronischen Transaktion unter Verwendung eines tragbaren Datenträgers anzugeben, das der Qualität der durchgeführten Nutzerauthentifizierung Rechnung trägt.

Diese Aufgabe wird gelöst durch ein Verfahren mit den Merkmalen des Hauptanspruchs. Die Aufgabe wird ferner gelöst durch einen tragbaren Datenträger, ein Terminal sowie ein System zur Durchführung einer gesicherten elektronischen Transaktion gemäß den unabhängigen Ansprüchen 20, 25 und 30.

Erfindungsgemäß wird bei der Ausführung einer Nutzerauthentifizierung von dem ausführenden Datenträger eine Qualitätsinformation über die eingesetzte Authentifizierungsmethode erzeugt. Dieser Beleg wird dem Ergebnis einer von dem tragbaren Datenträger nachfolgend ausgeführten sicherheitsbegründenden Operation beigefügt. Für den Empfänger einer so gebildeten Botschaft ist damit eindeutig erkennbar, auf welche Weise sich ein Nutzer vor Durchführung der sichheitsbegründenden Operation authentifiziert hat. Damit eröffnet sich dem Empfänger die Möglichkeit, die Ausführung einer gesicherten Transaktion von der Qualität der Nutzerauthentifizierung abhängig zu machen. So kann etwa bei einer Geldbörsenanwendung vorgesehen sein, daß die Entnahme eines unterhalb eines Grenzwertes liegenden Geldbetrags von einem Konto nach PIN-Authentifizierung erfolgen kann, die Entnahme von über dem Grenzwert liegenden Geldbeträgen dagegen nur nach Authentifizierung mittels eines biometrischen Merkmals.

Besonders vorteilhaft wird das erfindungsgemäße Verfahren im Rahmen der elektronischen Signatur eingesetzt.

In einer bevorzugten Ausführungsform ist die Durchführung der verschiedenen möglichen Nutzerauthentifizierungsmethoden so gestaltet, daß die Ausführungszwischenergebnisse der qualitativ niederwertigeren Methode nicht in einfacher Weise in Ausführungszwischenergebnisse einer qualitativ höherstehenden Methode überführt werden können. Damit wird erreicht, daß eine Manipulation eines Authentifizierungsbeleges selbst dann nicht möglich ist, wenn einem unberechtigten Nutzer sowohl ein tragbarer Datenträger wie eine zugehörige, niederwertige Authentisierungsinformation zur Verfügung steht, d. h. wenn ein unberechtigter Nutzer beispielsweise einen tragbaren Datenträger zusammen mit einer zugehörigen PIN besitzt.

Vorteilhaft werden weiter die bei der Durchführung einer Nutzerauthentifizierung jeweils nicht eingesetzten Authentifizierungsmethoden für die Dauer der Authentifizierung gesperrt.

Unter Bezugnahme auf die Zeichnung wird nachfolgend ein Ausführungsbeispiel der Erfindung näher erläutert.

Zeichnung

Es zeigen:

Figur 1 die Struktur eines Systems zur Vornahme einer digitalen Signatur,

Figuren 2, 3 den Ablauf der Durchführung einer digitalen Signatur als Flußdiagramm.

Figur 1 veranschaulicht die Grundstruktur eines Transaktionssystems zur Ausführung einer gesicherten elektronischen Transaktion. Wesentliche Elemente der Struktur im Hinblick auf die Erfindung sind ein Hintergrundsystem 10, das über ein Datennetz 12 mit einem Terminal 14 verbunden ist, ein tragbarer Datenträger 20, der von einem Nutzer 30 mitgeführt wird und zur Ausführung einer sicherheitsbegründenden Operation im Rahmen einer Transaktion eingerichtet ist, sowie ein Datensatz 40, der im Rahmen einer auszuführenden Transaktion sicher gehandhabt werden soll.

Für die gesicherte elektronische Transaktion wird im folgenden von einer Transaktion ausgegangen, welche die Erzeugung einer digitalen Signatur auf Seiten des Nutzers 30 erfordert. Eine solche Transaktion kann etwa die Durchführung eines Bankgeschäftes sein, bei dem das Konto des Nutzers 30 belastet wird. Die beschriebene Lösung ist aber nicht auf Transaktionen beschränkt, die eine digitale Signatur erfordern, sondern gundsätzlich in jeder Anwendung einsetzbar, bei der ein tragbarer Datenträger 20 von einem Terminal 14 zugeführte Datensätze 40 bearbeitet und an das Terminal 14 zurückgibt.

Das Hintergrundsystem 10 steht stellvertretend für eine Einrichtung, welche die eigentliche Transaktion vornimmt, etwa die Bewegung von Geld zwischen zwei Konten oder die Einleitung einer Warenauslieferung aufgrund einer Bestellung. Das Hintergrundsystem 10 kann entsprechend ein komplexes, aus vielen Einzelkomponenten bestehendes System sein oder auch, im Extremfall, gänzlich wegfallen. Ist die Transaktion eine Kontobewegungsanwendung, wird das Hintergrundsystem 10 typischerweise durch eine Bankzentrale gebildet.

Das Datennetz 12 dient zum Austausch von Daten zwischen einem Terminal 14 und dem Hintergrundsystem 10. Es kann jede beliebige physikalische Ausprägungsform besitzen und beispielsweise durch das Internet oder ein Mobilfunknetz realisiert sein.

Das Terminal 14 bildet die nutzerseitige Schnittstelle des Transaktionssystems und verfügt hierzu über Wiedergabemittel 16, typischerweise in Gestalt einer Bildanzeige, sowie Eingabemittel 18, etwa in Gestalt einer Tastatur. Das Terminal 14 kann ein öffentlich zugängliches Terminal, etwa ein in einer Bank aufgestelltes Gerät oder ein im Privatbereich eines Nutzers 30 befindliches Gerät, etwa ein PC oder ein Handy sein. Mit dem Datennetz 12, damit mit einem Hintergrundsystem 10 können ein oder mehrere Terminals 14 verbunden sein, die dabei von unterschiedlicher Bauart sein können. Das Terminal 14 verfügt über eine Schnittstelle 19 zur Kommunikation mit einem tragbaren Datenträger 20. Die Schnittstelle 19 kann von beliebiger physikalischer Ausführung, insbesondere von einem kontaktbehafteten oder von eine berührungslos arbeitenden Typ sein.

Das Terminal 14 besitzt ferner eine, im folgenden als Sensor bezeichnete, Sensoreinrichtung 15 zur Erfassung eines biometrischen Merkmales eines Nutzers 30. Durch den Sensor 15 erfaßbar sein können physiologische Merkmale, wie Gesichtsmerkmale, Merkmale des Auges oder Fingerabdrükke, oder verhaltensbasierte Merkmale wie etwa durch Stimme oder durch Schreibvorgänge ausgedrückte Sprech- oder Schriftsequenzen. In Fig.1 ist ein als Sensor 15 Fingerabdrucksensor angedeutet. Der Sensor 15 kann zur Aufnahme mehrerer verschiedener biometrischer Merkmale ausgebildet sein. Teil des Sensors 15 sind weiter Mittel zur Vorauswertung eines aufgenommenen biometrischen Merkmales. Dabei werden die aufgenommenen Informationen reduziert und auf bestimmte, charakteristische Primärmerkmale

zurückgeführt. Die verschiedenen Typen und die Durchführung biometrischer Authentifizierungsverfahren sind beispielsweise in dem eingangs genannten „Handbuch der Chipkarten", Kapitel 8.1.2, beschrieben.

Bei dem tragbaren Datenträger 20 handelt es sich beispielsweise um eine Chipkarte, wie sie in gleichfalls dem „Handbuch der Chipkarten" ausführlich beschrieben ist. Figur 1 deutet für den tragbaren Datenträger 20 insbesondere eine kontaktbehaftete Chipkarte mit einem Kontaktfeld 22 an, welches eine zu der terminalseitigen Schnittstelle 19 korrespondierende Schnittstelle bildet. Über die Schnittstellen 22, 19 erfolgt die Kommunikation zwischen Chipkarte 20 und Terminal 14. Außer der Gestalt einer Chipkarte kann der tragbare Datenträger 20 beliebige andere Gestaltungen aufweisen und beispielsweise in einem vom Nutzer 30 getragenen Bekleidungsstück oder einen vom Nutzer 30 mitgeführten Gebrauchsgegenstand realisiert sein.

Der tragbare Datenträger 20 besitzt einen integrierten Schaltkreis 24, welcher alle Elemente eines üblichen Computers aufweist, insbesondere einen Mikroprozessor 25 sowie Speichermittel 26. Der Mikroprozessor 25 ist zur Ausführung einer sicherheitsbegründenden Operation eingerichtet. Beispielsweise ist er dazu eingerichtet, einen zugeführten Datensatz 40, der im folgenden als elektronisches Dokument 40 bezeichnet wird, einem kryptographischen Algorithmus zu unterwerfen, wobei er wenigstens einen geheimen Schlüssel benutzt, der in den Speichermitteln 26 abgelegt ist. Der Mikroprozessor 25 ist ferner dazu eingerichtet, weitere Funktionalitäten gemäß in den Speichermitteln 26 abgelegten Programmen zu realisieren.

Der tragbare Datenträger 20 ist weiter zur Ausführung wenigstens eines, zweckmäßig jedoch mehrerer verschiedener Nutzerauthentifizierungsmethoden eingerichtet. Vorzugsweise unterstützt er wenigstens zwei im Hin-

blick auf die Qualität der Authentifizierung verschiedenwertige Authentifizierungmethoden. Zweckmäßig unterstützt er zumindest eine wissensbasierte Authentifizierungmethode, etwa eine PIN-Prüfung, sowie wenigstens eine biometrische Methode, in deren Rahmen ein am Terminal 14 zu präsentierendes biometrisches Merkmal des Nutzers 30 geprüft wird. Die biometrische Methode bildet hierbei die qualitativ höherwertige, da sie die persönliche Anwesenheit des Nutzers (30) voraussetzt; bei der wissenbasierten Methode ist dies nicht gewährleistet, das Wissen kann von einer unberechtigtem Nutzer erlangt worden sein. Entsprechend sind in den Speichermitteln 26 zumindest ein vom Nutzer 30 vorzulegendes Geheimnis, also etwa eine einem Benutzer 30 zugeordnete Referenz-PIN sowie wenigstens ein einem Benutzer 30 zugeordneter biometrischer Referenzdatensatz hinterlegt. Zweckmäßig kann vorgesehen sein, daß der tragbare Datenträger 20 mehr als zwei Authentifizierungsmethoden unterstützt, insbesondere weitere biometrische Methoden. Entsprechend sind in diesem Fall in den Speichermitteln 26 weitere Geheimnisse und/oder Referenzdatensätze hinterlegt und ist der integrierte Schaltkreis 24 dazu eingerichtet, die weiteren Authentifizierungsmethoden durchzuführen.

Nachfolgend wird anhand der Figuren 2 und 3 die Ausführung einer gesicherten elektronischen Transaktion unter Verwendung der in Figur 1 gezeigten Struktur beschrieben. Als sicherheitsbegründende Operation soll dabei ein elektronisches Dokument 40 signiert werden.

Eingeleitet wird die Nutzung durch Erstellung eines elektronischen Dokumentes 40 im Hintergrundsystem 10 oder im Terminal 14, Schritt 100. In der Regel geht der Erstellung ein auslösender Dialog zwischen einem Nutzer 30 und dem Hintergrundsystem 10 über das Terminal 14 voran. Spätestens wenn ein elektronisches Dokument 40 im Terminal 14 vorliegt, veranlaßt

dieses den Start der Signaturanwendung, Schritt 102. Die Startveranlassung kann dabei automatisch durch das Terminal 14 oder das Hintergrundsystem 10 erfolgen oder wird von dem Nutzer 30 eingeleitet, nachdem das Terminal 14 diesen dazu mittels einer geeigneten Darstellung auf der Anzeigevorrichtung 16 dazu aufgefordert hat.

Nachdem die Signaturanwendung gestartet wurde, präsentiert der Nutzer 30 dem Terminal 40 einen geeigneten tragbaren Datenträger 2o, Schritt 104. Für den tragbaren Datenträger 20 wird im folgenden die Gestalt einer kontaktbehafteten Chipkarte zugrunde gelegt. Weiter wird nachfolgend davon ausgegangen, daß die Chipkarte 20 zwei Authentifizierungsmethoden unterstützt, nämlich eine PIN-Prüfung als wissensbasierte, qualitativ niederwertige Methode, sowie eine Fingerabdruckprüfung als biometrische, qualitativ höherwertige Methode.

Hat das Terminal 14 die Anwesenheit einer Chipkarte 20 erkannt, führt es zunächst eine wechselseitige Authentisierung mit dieser durch, Schritt 106, wobei zunächst die Chipkarte 20 dem Terminal 14 die ihre, anschließend das Terminal 14 der Chipkarte 20 seine Authentizität nachweist.

Verläuft die Authentisierung erfolgreich, handeln Terminal 14 und Chipkarte 20 dynamische Sitzungsschlüssel aus, um die weitere Kommunikation gesichert im sogenannten „Secure Messaging"-Modus führen zu können, Schritt 108. Wegen Einzelheiten zum Konzept des Secure Messagings sowie dynamischen Sitzungsschlüsseln wird wiederum auf das „Handbuch der Chipkarten" verwiesen.

Anschließend erfolgt die Authentifizierung des Nutzers 30 gegenüber der Chipkarte 20. Hierbei prüft das Terminal 14 zunächst, auf welche Weise –

wissensbasiert, also durch Eingabe einer PIN oder biometrisch, d.h. durch Präsentation eines Fingerabdruckes - die Authentifizierung erfolgen soll, Schritt 110. Die Festlegung einer Authentifizierungsmethode kann aufgrund von mit dem elektronischen Dokument 40 übermittelten Informationen selbsttätig durch das Terminal 14 erfolgen, sie kann aber auch über die Anzeigevorrichtung 16 dem Nutzer 30 als Entscheidungsaufforderung vorgelegt werden. Im letzteren Fall trifft den Nutzer 30 mittels der Eingabemittel 18 eine Entscheidung.

Soll die Authentifizierung des Nutzers 30 wissensbasiert, d.h. durch Eingabe einer PIN erfolgen, sperrt die Chipkarte 20 die weiteren möglichen Authentifizierungsmethoden, d.h. die Fingerabdruckprüfung, Schritt 112, und fordert den Nutzer 30 über die Anzeigevorrichtung 16 auf, seine PIN über die Eingabemittel 18 einzugeben.

Der Nutzer 30 gibt daraufhin über die Eingabemittel 18 die PIN ein und das Terminal 14 leitet sie direkt oder abgewandelt über die Schnittstelle 19, 22 an die Chipkarte 20 weiter, Schritt 114. Die Übermittlung der PIN bzw. der daraus abgeleiteten Information wie die nachfolgend Kommunikation mit der Chipkarte wird zusätzlich unter Verwendung der ausgehandelten Sitzungsschlüssel gesichert. Zweckmäßig erfolgt die gesamte Kommunikation zwischen Terminal 14 und Chipkarte 20 im Secure Messaging Modus.

Diese prüft die übermittelte PIN und bestätigt im Gutfall dem Terminal 14 die Korrektheit, bzw. bricht das Verfahren ab, wenn die PIN als falsch geprüft wurde, Schritt 116.

Ist der Gutfall gegeben, veranlaßt das Terminal 14 die Chipkarte 20 durch entsprechend Befehle zur Durchführung der sicherheitsbegründenden Ope-

ration, d.h. der digitalen Signatur, und übermittelt der Chipkarte 20 das zu signierende elektronische Dokument 40, Schritt 118.

Die Chipkarte 20 signiert das zugeführte elektronische Dokument 40 mit dem in den Speichermitteln 22 gespeicherten geheimen Schlüssel, 120 und sendet die elektronische Signatur 40 zurück an das Terminal 14, Schritt 122, welches damit die eingeleitete elektronische Transaktion weiterführt.

Ergibt die Prüfung im Schritt 110, daß die Authentifizierung des Nutzers 30 nicht wissensbasiert sondern biometrisch erfolgen soll, leitet das Terminal 14 eine Authentifizierung gegen Präsentation eines biometrischen Merkmales ein und macht der Chipkarte 20 eine entsprechende Mitteilung, Schritt 130. Die Chipkarte 20 sperrt daraufhin die nun nicht eingesetzten weiteren Authentifizierungsmethoden, d.h. die wissensbasierten PIN-Prüfung, Schritt 132.

Nachfolgend präsentiert der Nutzer 30 dem Terminal 14 entsprechend der eingesetzten Authentifizierungsmethode ein biometrisches Merkmal, d.h. einen Fingerabdruck, Schritt 134. Die Aufforderung zur Präsentation des Fingerabdrucks erfolgt vorzugsweise durch eine entsprechende Darstellung auf der Anzeigevorrichtung 16 des Terminals 14. Der Fingerabdruck wird durch den am Terminal 14 vorgesehenen Sensor 15 erfaßt.

Das erfaßte biometrische Merkmal, d.h. den Fingerabdruck des Nutzers 30 unterwirft das Terminal 14 einer Vorverarbeitung, in der es aus dem am Sensor 15 gewonnenen Signal bestimmte kennzeichnende Merkmale extrahiert, Schritt 136. Bei Verwendung eines Fingerabdrucks werden beispielsweise Primärmerkmale des „Klassifikationsverfahrens nach Henry" ermittelt, wie es in dem „Handbuch der Chipkarten" beschrieben ist.

Die extrahierten Merkmale übermittelt das Terminal 14 über die Schnittstelle 19, 22 an den tragbaren Datenträger 20, Schritt 138.

Nach Eingang dort führt dieser eine Verifikation der übermittelten extrahierten Merkmale durch, Schritt 140. Hierbei vergleicht der integrierte Schaltkreis 24 die erhaltenen extrahierten Merkmale mit den in den Speichermitteln gespeicherten Referenzmerkmalen und prüft, ob eine hinreichende Übereinstimmung vorliegt. Ist das der Fall, bestätigt der tragbare Datenträger 20 dem Terminal 14 die erfolgreiche Verifikation des übermittelnden biometrischen Merkmales, Schritt 142. Weiter schaltet sich der tragbare Datenträger 20 zur Ausführung der beabsichtigte sicherheitsbegründenden Operation, d.h. zur Vornahme einer digitalen Signatur, bereit.

Nach Erhalt der Bestätigung über eine erfolgreiche Verifikation der Authentifizierung veranlaßt das Terminal 14 den Datenträger 20 durch entsprechende Befehle, die digitale Signatur auszuführen, Schritt 144. Zusammen mit den Befehlen übermittelt das Terminal 14 dem tragbaren Datenträger 20 dabei das zu signierende elektronische Dokument 40 oder zumindest Teile davon.

Der integrierte Schaltkreis 24 des tragbaren Datenträgers 20 führt daraufhin die zur Erstellung einer digitalen Signatur erforderlichen Operationen durch, Schritt 146. Typischerweise bildet er hierbei einen Hashwert über den erhaltenen Teil des elektronischen Dokuments 40 und verschlüsselt diesen mit einem in den Speichermitteln 26 gespeicherten, geheimen Schlüssel eines asymmetrischen, aus einem geheimen und eine öffentlichen Schlüssel bestehenden Schlüsselpaares.

Desweiteren bildet der integrierte Schaltkreis 24 eine Qualitätsinformation, Schritt 148, die quittiert, daß die Authentifizierung des Nutzers 30 unter Verwendung eines biometrischen Merkmales erfolgte. Diese Qualitätsinformation wird sodann fest mit der erstellten digitalen Signatur zu einer Sicherheitsbotschaft verknüpft, zweckmäßig im Rahmen des „Secure Messaging" Mechanismus unter Verwendung der zuvor ausgehandelten Sitzungsschlüssel.

Die so gebildete, aus digitaler Signatur und Qualitätsinformation bestehende Sicherheitsbotschaft sendet der tragbare Datenträger 20 zurück an das Terminal 14, Schritt 150. Von hier wird die übermittelte Sicherheitsbotschaft im Rahmen der ausgeführten gesicherten elektronischen Transaktion an den an der Transaktion beteiligten Empfänger, etwa ein Hintergrundsystem 10, weitergeleitet.

Zusätzlich zu der durch den tragbaren Datenträger 20 vorgenommenen sicherheitsbegründenden Operation erhält der Empfänger der Sicherheitsbotschaft dabei durch die darin enthaltene Qualitätsinformation eine Angabe über die Qualität der vorgenommenen Authentifizierung des Nutzers 30.

Im vorbeschriebenen Beispiel wurde eine Qualitätsinformation nur bei Verwendung einer biometrischen Authentifizierungsmethode erstellt, nicht bei Verwendung einer wissensbasierten Methode. Damit signalisiert bereits das Fehlen einer Qualitätsinformation die Verwendung einer qualtitativ niederwertigeren Methode. Selbstverständlich kann aber vorgesehen sein, daß die Bildung einer Qualitätsinformation grundsätzlich erfolgt, d.h. unabhängig davon, ob zur Authentifizierung eine wissensbasierte oder eine biometrische Methode gewählt wurde.

Unter Beibehaltung des grundlegenden Gedankens, dem Ergebnis einer von einem tragbaren Datenträger ausgeführten sicherheitsbegründenden Operation eine Qualitätsinformation über die Qualität der zuvor durchgeführten Nutzerauthentifizierung beizufügen, gestattet das vorbeschriebene Konzept weitere Ausgestaltungen und Abwandlungen. Dies gilt für die Gestaltung des bei der Ausführung einer Transaktion eingesetzten Systems, das mehr und Komponenten anderen Typs umfassen kann. Der beschriebene Verfahrensablauf kann ferner weitere Schritte, etwa Zwischenschritte umfassen.

## Patentansprüche

1. Verfahren zum Ausführen einer gesicherten elektronischen Transaktion an einem Terminal unter Verwendung eines tragbaren Datenträgers, wobei ein Nutzer sich gegenüber dem tragbaren Datenträger authentifiziert, der tragbare Datenträger dem Terminal den Nachweis der Authentifizierung bestätigt und der tragbare Datenträger anschließend im Rahmen der elektronischen Transaktion eine sicherheitsbegründende Operation ausführt, **dadurch gekennzeichnet**, daß der tragbare Datenträger (20) eine Qualitätsinformation darüber erstellt, auf welche Weise die Authentifizierung des Nutzers (30) erfolgte und diese Qualitätsinformation dem Ergebnis der sicherheitsbegründenden Operation beigefügt wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, daß die durch den tragbaren Datenträger (20) ausgeführte sicherheitsbegründende Operation in der Erstellung einer digitalen Signatur besteht.

3. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, daß die Authentifizierung des Nutzers (30) durch Präsentation eines biometrischen Merkmales vorgenommen wird.

4. Verfahren nach Anspruch 3, **dadurch gekennzeichnet**, daß die Authentifizierung des Nutzers (30) durch Präsentation eines für einen Nutzer (30) charakteristischen physiologischen oder verhaltensbasierten Merkmales vorgenommen wird.

5. Verfahren nach Anspruch 1 , **dadurch gekennzeichnet**, daß die Authentifizierung des Nutzers (30) durch Nachweis der Kenntnis eines Geheimnisses vorgenommen wird.

6. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, daß für die Authentifizierung des Nutzers (30) wenigstens zwei verschiedene Authentifizierungsmethoden von unterschiedlicher Qualität angeboten werden.

7. Verfahren nach Anspruch 6, **dadurch gekennzeichnet**, daß die jeweils nicht eingesetzten Authentifizierungsmethoden gesperrt werden.

8. Verfahren nach Anspruch 6, **dadurch gekennzeichnet**, daß für eine Authentifizierungsmethode keine Qualitätsinformation erzeugt wird.

9. Verfahren nach Anspruch 1 **dadurch gekennzeichnet**, daß ein Nutzer (30) zur Auswahl einer Authentifizierungsmethode aufgefordert wird.

10. Tragbarer Datenträger zur Ausführung einer sicherheitsbegründenden Operation im Rahmen einer gesicherten elektronischen Transaktion, wobei sich ein Nutzer gegenüber dem tragbaren Datenträger authentifiziert und der tragbare Datenträger einem Terminal die Authentifizierung bestätigt, **dadurch gekennzeichnet**, daß er dazu eingerichtet ist, eine Qualitätsinformation zu erstellen, welche angibt, auf welche Weise die Authentifizierung des Nutzers (30) durchgeführt wurde.

11. Datenträger nach Anspruch 10, **dadurch gekennzeichnet** daß der tragbare Datenträger (20) zur Erstellung einer digitalen Signatur eingerichtet ist.

12. Datenträger nach Anspruch 10, **dadurch gekennzeichnet** daß er wenigstens zwei qualitativ verschiedene Authentifizierungsmethoden unterstützt.

13. Terminal zur Verwendung in Verbindung mit einem tragbaren Datenträger nach Anspruch 9, **dadurch gekennzeichnet**, daß es Mittel aufweist (16,

18) aufweist, um einen Nutzer (30) zur Auswahl einer von wenigstens zwei möglichen Authentifizierungsmethoden zu veranlassen

14. System zur Ausführung einer gesicherten elektronischen Transaktion, in deren Rahmen die Qualität der Authentifizierung eines Nutzers gegenüber dem System festgestellt wird, umfassend einen tragbaren Datenträger nach Anspruch 10 sowie ein Terminal nach Anspruch 13.

**Fig. 1**

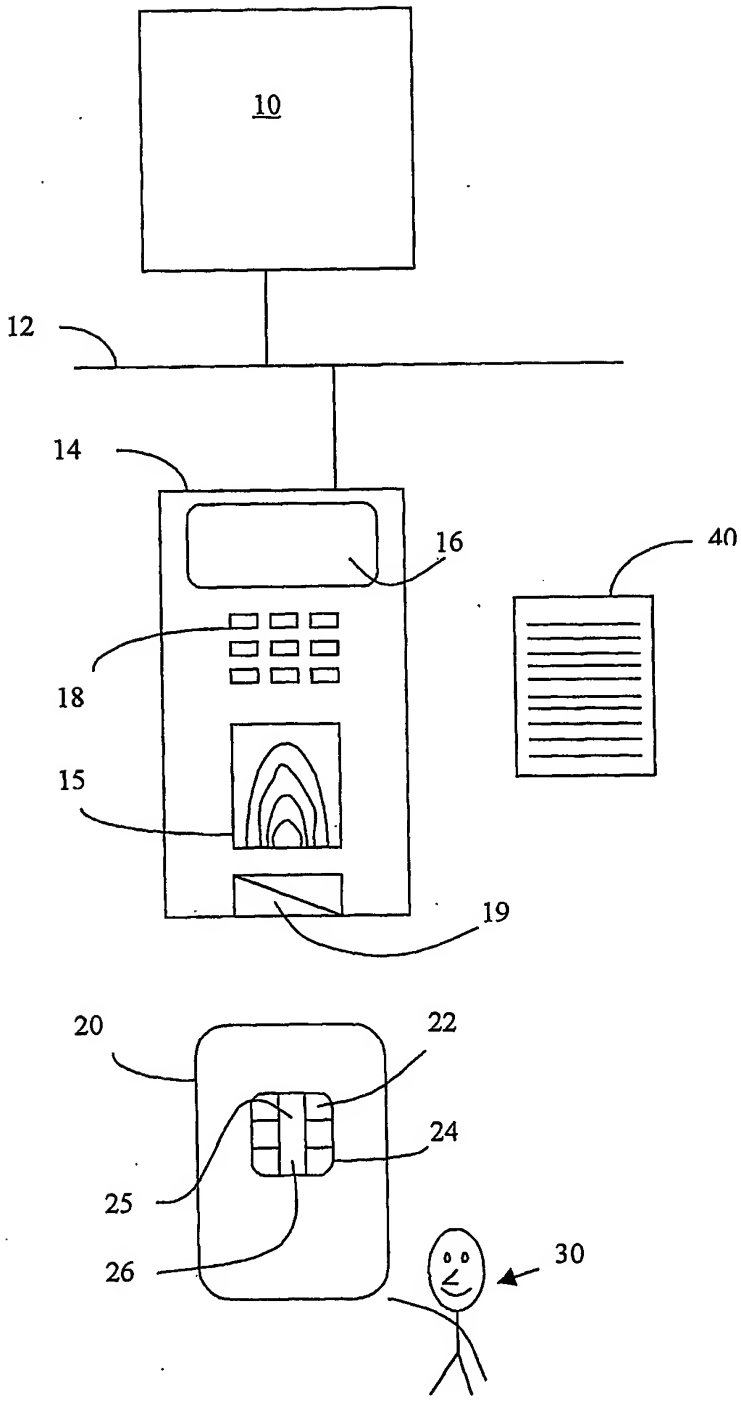


Fig. 2

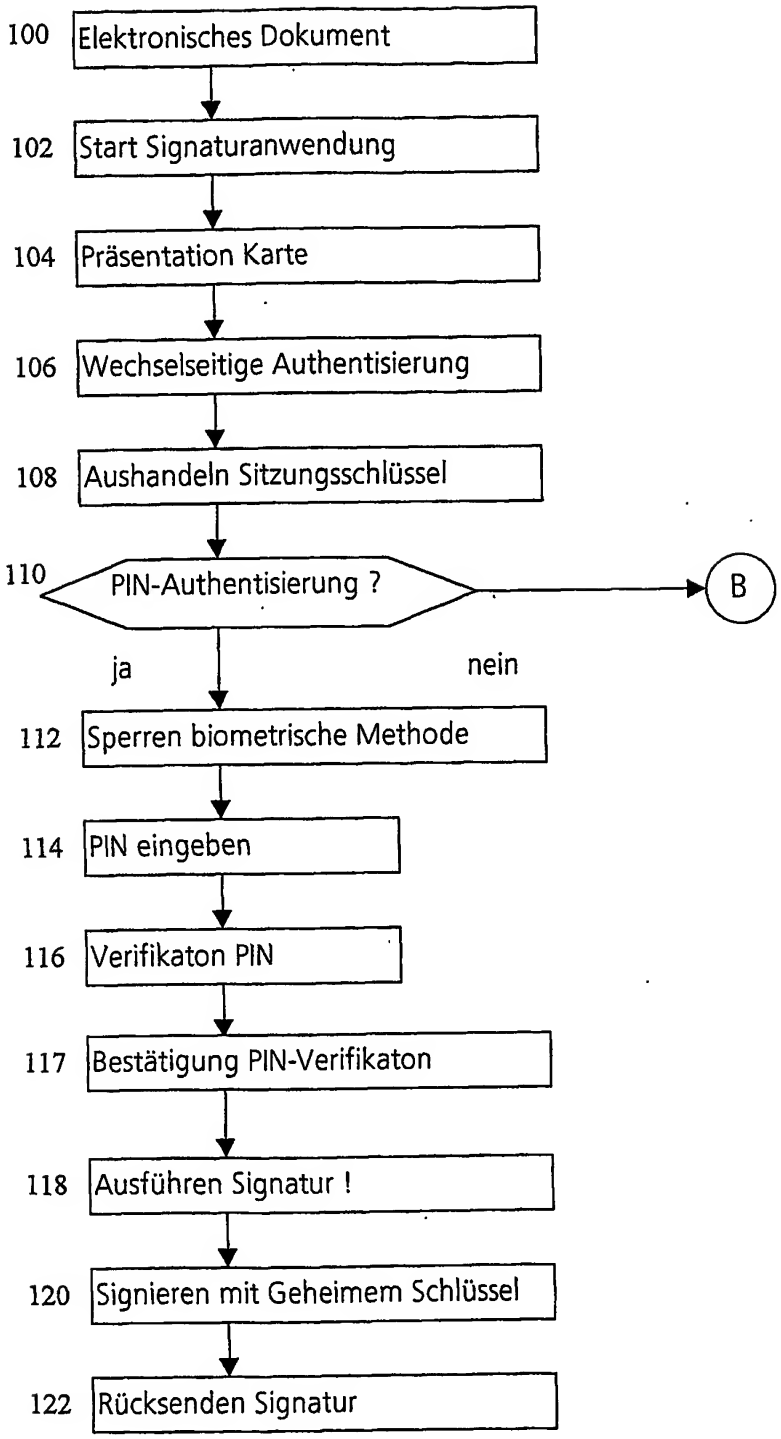
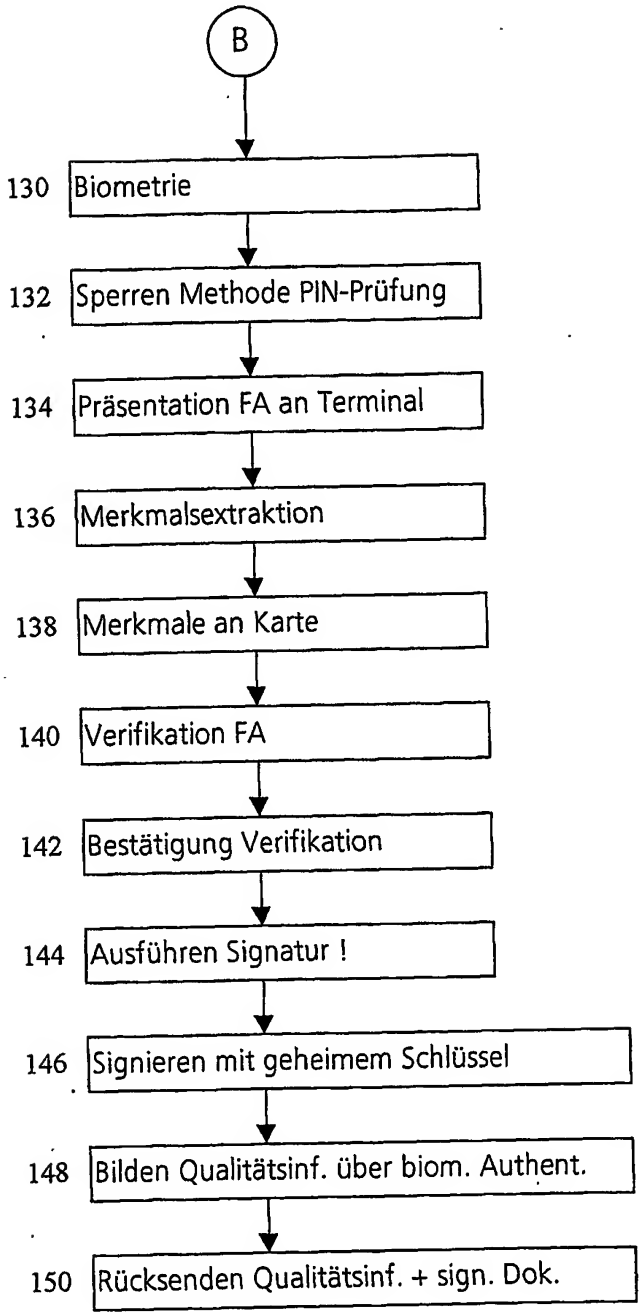

100
Elektronisches Dokument
102
Start Signaturanwendung
104
Präsentation Karte
106
Wechselseitige Authentisierung
108
Aushandeln Sitzungsschlüssel
110
PIN-Authentisierung ?
B
ja
nein
112
Sperren biometrische Methode
114
PIN eingeben
116
Verifikaton PIN
117
Bestätigung PIN-Verifikaton
118
Ausführen Signatur !
120
Signieren mit Geheimem Schlüssel
122
Rücksenden Signatur

Fig. 3


B
130 Biometrie
132 Sperren Methode PIN-Prüfung
134 Präsentation FA an Terminal
136 Merkmalsextraktion
138 Merkmale an Karte
140 Verifikation FA
142 Bestätigung Verifikation
144 Ausführen Signatur !
146 Signieren mit geheimem Schlüssel
148 Bilden Qualitätsinf. über biom. Authent.
150 Rücksenden Qualitätsinf. + sign. Dok.

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/11761

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y<br>A | EP 1 045 346 A (OMRON CORPORATION)<br>18 October 2000 (2000-10-18)<br>abstract; claims; figures<br>paragraph '0010! - paragraph '0020! | 1,3,4,6,<br>10,12,14<br>7 |
| Y<br>A | US 4 993 068 A (G.V. PIOSENKA ET AL.)<br>12 February 1991 (1991-02-12)<br>abstract; claims; figures<br>column 10, line 28 - line 40 | 1,3,4,6,<br>10,12,14<br>5,8 |
| A | US 6 263 447 B1 (J. FRENCH)<br>17 July 2001 (2001-07-17)<br>abstract; claims; figures 12,45<br>column 2, line 57 -column 3, line 11<br>column 5, line 12 -column 6, line 42<br>column 12, line 14 - line 63 | 1,3-6,<br>10,12,14 |

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 19 February 2004 | 26/02/2004 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,<br>Fax: (+31–70) 340–3016 | David, J |

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/11761

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | US 6 408 388 B1 (A.M. FISCHER)<br>18 June 2002 (2002-06-18)<br>abstract; claims; figures | 1,2,5,<br>10,11,14 |
| A | WO 01 82190 A (GLOBAL TRANSACTION COMPANY)<br>1 November 2001 (2001-11-01) | |
| A | WO 02 067091 A (ISHOPSECURE)<br>29 August 2002 (2002-08-29) | |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 03/11761

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| EP 1045346 A | 18-10-2000 | JP 2000268175 A | 29-09-2000 |
| | | EP 1045346 A2 | 18-10-2000 |
| US 4993068 A | 12-02-1991 | NONE | |
| US 6263447 B1 | 17-07-2001 | US 2003033526 A1 | 13-02-2003 |
| | | US 6496936 B1 | 17-12-2002 |
| | | US 2002157029 A1 | 24-10-2002 |
| | | AU 4091199 A | 06-12-1999 |
| | | CA 2356998 A1 | 25-11-1999 |
| | | EP 1080415 A1 | 07-03-2001 |
| | | WO 9960483 A1 | 25-11-1999 |
| US 6408388 B1 | 18-06-2002 | US 5936149 A | 10-08-1999 |
| | | US 5422953 A | 06-06-1995 |
| | | US 2003041246 A1 | 27-02-2003 |
| | | AT 196582 T | 15-10-2000 |
| | | AT 205309 T | 15-09-2001 |
| | | AU 666424 B2 | 08-02-1996 |
| | | AU 5778194 A | 17-11-1994 |
| | | CA 2120665 A1 | 06-11-1994 |
| | | DE 69425923 D1 | 26-10-2000 |
| | | DE 69425923 T2 | 18-01-2001 |
| | | DE 69428215 D1 | 11-10-2001 |
| | | DE 69428215 T2 | 18-04-2002 |
| | | DK 624014 T3 | 04-12-2000 |
| | | EP 0624014 A2 | 09-11-1994 |
| | | EP 0770953 A2 | 02-05-1997 |
| | | EP 0841604 A2 | 13-05-1998 |
| | | ES 2149843 T3 | 16-11-2000 |
| | | GR 3034459 T3 | 29-12-2000 |
| | | JP 7254897 A | 03-10-1995 |
| | | PT 624014 T | 29-12-2000 |
| WO 0182190 A | 01-11-2001 | AU 5379501 A | 07-11-2001 |
| | | WO 0182190 A1 | 01-11-2001 |
| WO 02067091 A | 29-08-2002 | US 2002116333 A1 | 22-08-2002 |
| | | EP 1364274 A2 | 26-11-2003 |
| | | WO 02067091 A2 | 29-08-2002 |

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 03/11761

**A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**
IPK 7 G07F7/10

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

**B. RECHERCHIERTE GEBIETE**

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

**C. ALS WESENTLICH ANGESEHENE UNTERLAGEN**

| Kategorie° | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| Y<br>A | EP 1 045 346 A (OMRON CORPORATION)<br>18. Oktober 2000 (2000-10-18)<br>Zusammenfassung; Ansprüche; Abbildungen<br>Absatz '0010! - Absatz '0020! | 1,3,4,6,<br>10,12,14<br>7 |
| Y<br>A | US 4 993 068 A (G.V. PIOSENKA ET AL.)<br>12. Februar 1991 (1991-02-12)<br>Zusammenfassung; Ansprüche; Abbildungen<br>Spalte 10, Zeile 28 - Zeile 40 | 1,3,4,6,<br>10,12,14<br>5,8 |
| A | US 6 263 447 B1 (J. FRENCH)<br>17. Juli 2001 (2001-07-17)<br>Zusammenfassung; Ansprüche; Abbildungen<br>12,45<br>Spalte 2, Zeile 57 -Spalte 3, Zeile 11<br>Spalte 5, Zeile 12 -Spalte 6, Zeile 42<br>Spalte 12, Zeile 14 - Zeile 63 | 1,3-6,<br>10,12,14 |

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

| Datum des Abschlusses der internationalen Recherche | Absendedatum des internationalen Recherchenberichts |
|---|---|
| 19. Februar 2004 | 26/02/2004 |

| Name und Postanschrift der Internationalen Recherchenbehörde | Bevollmächtigter Bediensteter |
|---|---|
| Europäisches Patentamt, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | David, J |

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 03/11761

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie° | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| A | US 6 408 388 B1 (A.M. FISCHER)<br>18. Juni 2002 (2002-06-18)<br>Zusammenfassung; Ansprüche; Abbildungen | 1,2,5,<br>10,11,14 |
| A | WO 01 82190 A (GLOBAL TRANSACTION COMPANY)<br>1. November 2001 (2001-11-01) | |
| A | WO 02 067091 A (ISHOPSECURE)<br>29. August 2002 (2002-08-29) | |

## INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 03/11761

| Im Recherchenbericht angeführtes Patentdokument | | Datum der Veröffentlichung | Mitglied(er) der Patentfamilie | | Datum der Veröffentlichung |
|---|---|---|---|---|---|
| EP 1045346 | A | 18-10-2000 | JP | 2000268175 A | 29-09-2000 |
| | | | EP | 1045346 A2 | 18-10-2000 |
| US 4993068 | A | 12-02-1991 | KEINE | | |
| US 6263447 | B1 | 17-07-2001 | US | 2003033526 A1 | 13-02-2003 |
| | | | US | 6496936 B1 | 17-12-2002 |
| | | | US | 2002157029 A1 | 24-10-2002 |
| | | | AU | 4091199 A | 06-12-1999 |
| | | | CA | 2356998 A1 | 25-11-1999 |
| | | | EP | 1080415 A1 | 07-03-2001 |
| | | | WO | 9960483 A1 | 25-11-1999 |
| US 6408388 | B1 | 18-06-2002 | US | 5936149 A | 10-08-1999 |
| | | | US | 5422953 A | 06-06-1995 |
| | | | US | 2003041246 A1 | 27-02-2003 |
| | | | AT | 196582 T | 15-10-2000 |
| | | | AT | 205309 T | 15-09-2001 |
| | | | AU | 666424 B2 | 08-02-1996 |
| | | | AU | 5778194 A | 17-11-1994 |
| | | | CA | 2120665 A1 | 06-11-1994 |
| | | | DE | 69425923 D1 | 26-10-2000 |
| | | | DE | 69425923 T2 | 18-01-2001 |
| | | | DE | 69428215 D1 | 11-10-2001 |
| | | | DE | 69428215 T2 | 18-04-2002 |
| | | | DK | 624014 T3 | 04-12-2000 |
| | | | EP | 0624014 A2 | 09-11-1994 |
| | | | EP | 0770953 A2 | 02-05-1997 |
| | | | EP | 0841604 A2 | 13-05-1998 |
| | | | ES | 2149843 T3 | 16-11-2000 |
| | | | GR | 3034459 T3 | 29-12-2000 |
| | | | JP | 7254897 A | 03-10-1995 |
| | | | PT | 624014 T | 29-12-2000 |
| WO 0182190 | A | 01-11-2001 | AU | 5379501 A | 07-11-2001 |
| | | | WO | 0182190 A1 | 01-11-2001 |
| WO 02067091 | A | 29-08-2002 | US | 2002116333 A1 | 22-08-2002 |
| | | | EP | 1364274 A2 | 26-11-2003 |
| | | | WO | 02067091 A2 | 29-08-2002 |